Patent
Attorney's Docket No. 031941-094

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Peter YEUNG et al.	)	Group Art Unit: Unassigned
	)	
Application No.: Unassigned	)	Examiner: Unassigned
	)	
Filed: October 12, 2001	)	
	)	
For: System and Method Relating to Access Control	)	

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination, please amend this application as follows.

IN THE CLAIMS

Please delete claims 1-34 and add new claims 34-68 as follows.

35. A system for end-user control of a distribution and maintenance of end-user personal profile data in a data communications system providing communication between applications having or communicating with service, information, or content providers or holding means having end-user personal profile data, the system comprising:

a personal profile protection network with at least one central protection server means having or communicating with an information holding means holding personal protection profile information, and

a number of distributed access means,

wherein for each of said applications at least one access means is provided, a granting or rejecting of an access request for end-user personal profile data by a requesting application is determined by the central protection server in communication with at least one of a requesting application and an information providing application, translating means are provided for identity translation, an

identity of a requesting application will be concealed an information providing application, and an identity of an information providing applications will be concealed from a requesting application.

36. The system according to claim 35, wherein there is one access means for each application.

37. The system according to claim 35, wherein there are a plurality of access means for at least one application.

38. The system according to claim 35, wherein the central server means only includes personal protection profile data, the personal profile data being distributed throughout the system.

39. The system according to claim 38, wherein the personal protection profile data includes information for each end-user of the system about which end-user personal profile data are accessible by a given application.

40. The system according to claim 38, wherein the personal protection profiles are assigned one of a number of security levels, a lowest security level indicating that all personal profile data access is prevented for every application, and a highest security level indicating that all personal profile data is freely available.

41. The system according to claim 35, wherein an interface between an application and respective access means comprises an Application Programmable Interface based on a generic markup language.

42. The system according to claim 41, wherein the generic markup language is XML.

43. The system according to claim 41, wherein access to requested end-user personal profile data is granted or rejected by the central server in communication with the requesting application.

44. The system according to claim 41, wherein access to requested end-user personal profile data is granted or rejected by the central server in communication with the information providing application.

45. The system according to claim 41, wherein access to requested end-user personal profile data is granted or rejected by the central server in communication with the requesting application and the information providing application.

46. The system according to claim 43, wherein first user identity translating means are provided at least in the central server means.

47. The system according to claim 44, wherein second user identity translating means are provided in the access means of the requesting application.

48. The system according to claim 41, wherein for each pair of applications of the system a general Document Type Definition (DTD) is given to define an allowed flow of personal data.

49. The system according to claim 48, wherein for each user a specific user DTD agreement is given.

50. The system according to claim 41, wherein an access request for end-user profile data is transported from the requesting application to its access means using Remote Method Invocation (RMI), and the access request includes a user identity associated with the requested personal end-user profile.

51. The system according to claim 50, wherein the request is transported as an XML transport object tagged with information about the requested end-user personal profile data.

52. The system according to claim 50, wherein a HTTPS protocol is used for communication between the access means of the requesting or information holding application and the central server means.

53. The system according to claim 35, wherein the access means of the information requesting or providing application includes means for encrypting the user identity associated with the requested end-user profile.

54. The system according to claim 35, wherein the request is digitally signed with at least one of a private key of the access means of the requesting application and a private key of the access means of the information providing application.

55. The system according to claim 54, wherein the request is digitally signed with a private key of the central server means, and a digital signature of the access means are verified in the central server means.

56. The system according to claim 55, wherein the central server means comprises means for encrypting at least the user identity associated with the requested information used by the information providing information.

57. The system according to claim 35, wherein at least some of the applications include respective cache memory for temporarily holding information about access requests, and a previously used session can be reused at least for a given time period.

58. A personal profile control network for controlling the access to personal profile data, comprising:

at least one central protection server means having or communicating with information holding means having personal protection profile information, and

a number of distributed access means, at least one access means respectively interfacing with each of a number of applications,

wherein the central protection server means further comprises means for translating and verifying identities, a request for access to personal profile data by a requesting application is communicated to the requesting application access means and is granted or rejected by the central server means in communication with the access means of the requesting application or the information providing application, and the user identity used by the requesting application is concealed for the information providing application and an identity of an information providing application will be concealed from a requesting application.

59. The personal profile control network according to claim 58, wherein an interface between an application and respective access means is based on a generic mark-up language.

60. The personal profile control network according to claim 59, wherein the generic mark-up language is XML

61. The personal profile control network according to claim 58, wherein the information holding means of the central server means comprises a personal protection profile for each user of the system and the personal protection profiles are end-user controlled.

62. The personal profile control network according to claim 61, wherein the central server means and at least one of the information requesting and providing

access means digitally sign a request for personal profile data with a respective private key, and digital signatures are verified by the central server means.

63. A method of controlling access to personal data within a personal end-user profile in a data communication network running a number of applications having or communicating with information holding means, the method comprising the steps of:

providing an access request from a requesting application to an access means associated with a requesting application using a generic mark-up language,

forwarding the access request from the access means to a central server means having information having means holding personal protection profiles for end-users in the system;

performing user identification encryption, the user identification of the requesting application being concealed from an information providing application, and an identity of an information providing application will be concealed from a requesting application;

establishing whether access is to be granted or denied by using the request and the personal protections profile,

if access to the requested personal profile is to be granted, confirming to the access means of the requesting application that access is to be granted after digitally signing the request; and

allowing transfer of the encrypted and digitally signed request to the information providing application.

64. The method according to claim 63, wherein the access request of a requesting application relates to accessing data in a personal profile, and for a granted request, the method further comprises the step of:

transferring the requested data via the access means of an information providing application over a data communication network to the access means of the requesting application.

65. The method according to claim 63, wherein the access request of a requesting application relates to setting or updating data in a personal profile, and for a granted request, the method further comprises the step of:

transferring the data to be set or updated to the information providing application over the data communication network.

66. A method of controlling access to personal data within a personal end-user profile in a data communication network running a number of applications having or communicating with information holding means, the method of comprising the steps of:

forwarding a request for access to data within a personal profile from a requesting application via at least one distributed access means to a central server means;

establishing in the central server means whether access to requested data should be allowed or not by comparing the request with an end-user controlled personal protection profile; and

providing the at least one distributed access means with information as to whether access is allowable or not, such that if access is allowable, the data communication network can be used for giving the requesting application access to the requested data without the identity of the requesting application being visible to the application able to provide access to the requested data, and an identity of an information providing application will be concealed from a requesting application.

67. The method according to claim 66, further comprising the steps of:

encrypting at least one of a user identity associated with the requested end-user profile into the request at the central server means and the access means associated with the requesting application; and

decrypting the user identity at the access means associated with the information providing application.

68. The method according to claim 66, further comprising the steps of:

digitally signing the request at one or more of the access means associated with the information requesting application, the access means associated with the information providing application and the central server means, the access means and the central server means comprising a personal profile data protection network.

IN THE ABSTRACT

Please REPLACE the Abstract on page 47 and insert the new Abstract attached as a separate sheet.

REMARKS

The specification and Abstract have been amended and the claims have been replaced to place the application in better form for examination. Favorable consideration is respectfully solicited.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By: STEPHEN J. TYTKAN; Reg. #45,846
Michael G. Savage
Registration No. 32,596

P.O. Box 1404
Alexandria, Virginia 22313-1404
(919) 941-9240

Dated: October 12, 2001

"Express Mail" mailing label No. EL766105629US
Date of Deposit 10/12/01
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

H. Rattelade
(Type or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

ABSTRACT

A system for end-user control of the distribution and maintenance of end-user personal profile data in a data communications system providing communication between applications comprising and/or communicating with service, information, or content providers or holding end-user personal profile data is presented. The system includes a personal profile protection network with at least one central protection server module having or communicating with an apparatus for holding personal protection profile information, and a number of distributed access modules. For each of the applications, at least one access module is provided, and a granting or rejecting of an access request for end-user personal profile data by a requesting application is determined by the central protection server in communication with a requesting application or an information providing application. Translators are provided for identity translation and the identity of a requesting application will be concealed from an information providing application, and an identity of an information providing application will be concealed from a requesting application.